

So macht man die Cloud sicher!

Über 60 Prozent aller Unternehmen planen heute, Cloud-basierende Angebote innerhalb der kommenden 18 Monate zu evaluieren oder Pilotprojekte zu starten¹. Für viele Anwendungen ist das SaaS-Modell inzwischen der Quasi-Standard, etwa bei Sales-Force Automation, Projektmanagement oder Marketing-Automation. Betrachtet man jedoch die letztendlichen Möglichkeiten dieser Technologie, stellen diese ersten Cloud-Initiativen für viele Unternehmen nur den berühmten Tropfen auf den heißen Stein dar.



Pius Graf

Regional Sales Director
SafeNet Schweiz

So etwa im Falle eines grossen, multinationalen Handelsunternehmens. Dieses suchte nach einem Weg, seine virtuellen Maschinen während der Weihnachtszeit auf Cloud-basierende Ressourcen zu verlagern. Da der Händler 70 Prozent seines Umsatzes in diesen vier Wochen erwirtschaftet, lassen sich so die operativen Kosten der IT für die weniger umsatzstarke Zeit spürbar senken und damit Millionen im Prozess sparen.

Es sind diese strategischen Initiativen, durch die Unternehmen die Vorteile der Cloud - Elastizität und geringere Kosten - in vollem Umfang realisieren. Jedoch ist eine entscheidende Hürde zu meistern, bevor diese Vision zur Realität werden kann: In der Cloud müssen Sicherheit, Vertrauenswürdigkeit und Kontrolle sichergestellt sein. Welche Vorkehrungen haben die Cloud-Anbieter getroffen, um vor Schwachstellen gefeit zu sein? Wie können die Unternehmen sicherstellen, dass ihre sensiblen Daten in der virtualisierten, von mehreren Kunden gemeinsam genutzten Umgebung nicht versehentlich mit den Daten eines anderen Unternehmens vermischt werden? Und wie können die Unternehmen die Einhaltung der gesetzlichen Vorgaben bei den eingesetzten Cloud-Diensten garantieren und nachweisen?

Mit diesen Aspekten kämpfen heute Unternehmen, die mehrere Cloud-Initiativen verfolgen.

security-zone 2011

So schaffen Sie Vertrauen ins Cloud Computing

Mehr dazu im Referat von Pius Graf am Dienstag 11. Oktober um 08.00 Uhr

Details & Anmeldung [hier ...](#)

Und je mehr die strategische Bedeutung des Cloud-Engagements wächst, desto wichtiger wird auch die Sicherheit. Die zunehmenden Sicherheitsansprüche erfordern grössere Aufwände und Investitionen sowohl der Unternehmen als auch der Security-Anbieter. Darum erwartet Forrester, dass der Markt für Cloud-Security innerhalb der kommenden 5 Jahre auf 1,5 Milliarden Dollar klettern wird².

¹ Gartner: "Hype Cycle for Cloud Computing, 2010". David Mitchell Smith, 27. Juli 2010

² Forrester Research: "Security And The Cloud: Looking At The Opportunity Beyond The Obstacle". Jonathan Penn mit Heidi Shey, Christopher Mines, Chétina Muteba, 20. Oktober 2010

Verschlüsselung: Grundlegende Kontrolle für die Cloud

Bevor Anwender strategisch wichtige Dienste in die Cloud verlagern können, müssen sie in der Lage sein, Cloud-Dienste unter Beibehaltung ihrer Sicherheitsmechanismen zu nutzen. Dabei wird von Sicherheitsexperten und Marktbeobachtern die Verschlüsselung immer mehr als ein grundlegendes Security-Werkzeug angesehen. Verschlüsselung – richtig eingeführt mit den entsprechenden Ansätzen beim sicheren Key- und Richtlinien-Management – ermöglicht es, Daten und zugehörige Regelwerke zu isolieren. Das ist besonders in mandantenfähigen Umgebungen wichtig. Mit dieser Technologie können Unternehmen Cloud-Dienste nutzen, ohne Kompromisse bei Sicherheit und Compliance einzugehen.

Verschlüsselung ist bereits in herkömmlichen Rechenzentren eine kritische Sicherheitskomponente; in der Cloud steigt ihre strategische Bedeutung nochmals erheblich. Bislang erlaubten es physische Sicherheitsmechanismen, physische Trennung und die grundsätzliche Vertrauenswürdigkeit im Rechenzentrum, in manchen Bereichen auf Verschlüsselung zu verzichten. In der Cloud verschwinden diese physischen Barrieren und Vertrauenspositionen vollständig. Die Verschlüsselung wird somit deutlich wichtiger und tritt an deren Stelle.

Was ist nun von Organisationen zu beachten, die Daten in die Cloud verlagern wollen?

• Sicherheit und Compliance müssen auch in der Cloud gewährleistet sein.

Sicherheitslösungen müssen ein komplettes Geflecht aus durchgängigem Schutz, flexibler Verschlüsselung, verankerten Identitäten und sicherer Kommunikation sein. Dadurch bekommen die Organisationen die Möglichkeit, auch in mandantenfähigen Cloud-Umgebungen jederzeit die Kontrolle darüber zu behalten, wie Daten isoliert, geschützt und geteilt werden.

• Einen konkreten Migrationspfad in die Cloud umsetzen.

Sicherheitslösungen müssen eine modulare Architektur haben. Damit erhalten Unternehmen die Flexibilität, auf möglichst effiziente und effektive Art auf Cloud Computing zu migrieren – entsprechend den individuellen Zeitvorstellungen, Geschäftszielen und Sicherheitsrichtlinien. Sie müssen es möglich machen, dass Unternehmen ihre dringlichsten Sicherheitsanforderungen sowohl kurz- als auch langfristig umsetzen. Egal, ob sicherer Zugriff auf SaaS-Anwendungen, verschlüsselter Speicherplatz in der Cloud, geschützte Kommunikation zwischen Public und Private Cloud oder andere Ziele erreicht werden müssen.

• Die Vorteile der Cloud vollständig ausschöpfen.

Sicherheitslösungen müssen extrem leistungsfähig sein und extra für den Einsatz in virtualisierten Umgebungen entwickelt worden sein. Zudem müssen sie ermöglichen sensible Daten und Anwendungen über Cloud- sowie Rechenzentrumsgrenzen hinweg zentral zu verwalten und zu steuern. Dadurch erreichen die Administrationsteams die optimale Effizienz, das Unternehmen kann die Möglichkeiten des Cloud Computings bedenkenlos nutzen.

Bestandteile einer sicheren Cloudstrategie

Bei den Cloud-Initiativen eines Unternehmens gibt es keinen goldenen Standardweg für alle Szenarien. Viele Unternehmen werden verschiedene, mehrgleisige Ansätze für Cloud Computing wählen. Damit benötigen sie eine modulare Lösung, die flexible Integrationspunkte für Public, Private und hybride Clouds bietet. SafeNet verfügt über ein vollständiges Portfolio an Lösungen, die den Unternehmen die benötigten Merkmale bereit stellen, sobald sie gebraucht werden. Unabhängig davon, wo das Unternehmen bei der Umsetzung seiner Cloud-Strategie steht.